

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A content playback device for decrypting encrypted content recorded on a recording medium and playing back the decrypted content, comprising:

a read unit operable to read media information unique to the recording medium, from the recording medium;

a judgment unit operable to acquire, from a source other than the recording medium, contract information relating to a contract for use of the encrypted content, and judge, based on the acquired contract information, whether the encrypted content is permitted to be used;

a reception unit operable to receive a designation of the encrypted content;

an acquisition unit operable to acquire protection method information showing one of a first protection method and a second protection method that is used for protecting the encrypted content;

a generation unit operable to generate a content key, corresponding to the acquired protection method information, based on the read media information and the acquired contract information, if the encrypted content is judged as being permitted to be used;

a decryption unit operable to read the encrypted content from the recording medium, and decrypt the encrypted content using the generated content key; and

a playback unit operable to play back the decrypted content, wherein the encrypted content includes at least first-type encrypted content that is protected by the first protection method and a second-type encrypted content that is protected by the second protection method different from the first protection method.

2. (Original) The content playback device of Claim 1, wherein
the media information shows a media key which is assigned to the recording medium,
the contract information shows a license key which is assigned to the contract, and
the generation unit generates the content key based on the media key shown by the media information and the license key shown by the contract information.

3. (Original) The content playback device of Claim 2, wherein
the contract information includes a use condition of the encrypted content, and

the judgment unit judges whether the encrypted content is permitted to be used, based on the use condition included in the contract information.

4. (Original) The content playback device of Claim 2, wherein the recording medium stores generation method information in correspondence with the encrypted content, the generation method information showing whether the content key is to be generated using the license key, using the media key, or using both the license key and the media key, and

the generation unit reads the generation method information from the recording medium, and generates the content key according to the read generation method information.

5. (Original) The content playback device of Claim 4, wherein if the generation method information shows that the content key is to be generated using both the license key and the media key, the generation unit applies a one-way function to the license key and the media key to generate the content key.

6. (Original) The content playback device of Claim 4, wherein the contract information includes the license key, as the content key, which has been encrypted using the media key, and

if the generation method information shows that the content key is to be generated using both the license key and the media key, the generation unit decrypts the encrypted license key using the media key to generate the content key.

7. (Original) The content playback device of Claim 2, wherein the media information includes the media key which has been encrypted, and the generation unit decrypts the encrypted media key to obtain the media key.

8. (Original) The content playback device of Claim 7, wherein the media key has been encrypted using device information unique to the content playback device, and the generation unit reads the device information held in the content playback device, and

decrypts the encrypted media key using the read device information.

9. (Original) The content playback device of Claim 2, wherein
the recording medium stores a contract identifier for identifying the contract information,
in correspondence with the encrypted content, and
the judgment unit reads the contract identifier from the recording medium, and acquires
the contract information identified by the read contract identifier.

10. (Original) The content playback device of Claim 2, wherein
the recording medium stores a content identifier for identifying the encrypted content,
and
the judgment unit reads the content identifier from the recording medium, and acquires
the contract information corresponding to the read content identifier.

11. (Original) The content playback device of Claim 2, wherein the
judgment unit includes:
a storage unit operable to store the contract information beforehand; and
a judging unit operable to read the contract information from the storage unit, and judge,
based on the read contract information, whether the encrypted content is permitted to be used.

12. (Original) The content playback device of Claim 2, wherein
the contract information is stored on another recording medium, in correspondence with
the encrypted content, and
the judgment unit acquires the contract information by reading the contract information
from the other recording medium.

13. (Original) The content playback device of Claim 2 being connected, via a network,
to a server device for delivering the contract information, wherein the judgment unit acquires
the contract information by receiving the contract information from the server device.

14. (Original) The content playback device of Claim 2, wherein the generation unit is

constituted by a removable module.

15. (Original) The content playback device of Claim 14, wherein
the generation unit and the judgment unit perform mutual authentication,
the judgment unit outputs the contract information to the generation unit, if the
judgment unit has succeeded in authenticating the generation unit, and
the generation unit receives the contract information from the judgment unit and
generates the content key, if the generation unit has succeeded in authenticating the
judgment unit.

16. (Original) The content playback device of Claim 15, wherein the generation unit
stores a first module identifier for identifying an invalid module, acquires an identifier for
identifying the judgment unit compares the acquired identifier with the first module identifier,
and refuses to receive the contract information from the judgment unit if the acquired identifier
matches the first module identifier.

17. (Original) The content playback device of Claim 16, wherein
the recording medium stores a second module identifier for identifying an invalid
module, and
the judgment unit reads the second module identifier from the recording medium,
acquires an identifier for identifying the generation unit, compares the acquired identifier with
the second module identifier, and refuses to output the contract information to the generation unit
if the acquired identifier matches the second module identifier.

18. (Cancelled)

19. (Currently Amended) The content playback device of ~~Claim 18~~Claim 19, wherein
the first protection method uses a media key assigned to the recording medium, and the
second protection method uses a license key assigned to a contract for use of the encrypted
content, and
the generation unit uses the media key to generate the content key if the protection

method information shows the first protection method, and uses the license key to generate the content key if the protection method information shows the second protection method.

20. (Original) The content playback device of Claim 19, wherein
the recording medium stores the protection method information in correspondence with
the encrypted content, and
the acquisition unit acquires the protection method information by reading the protection
method information from the recording medium.

21. (Original) The content playback device of Claim 19, further comprising a
judgment unit operable to acquire contract information relating to the contract, and judge,
based on the acquired contract information, whether the encrypted content is permitted to be
used,
wherein the generation unit generates the content key if the encrypted content is judged
as being permitted to be used.

22. (Original) The content playback device of Claim 19, wherein
the protection method information includes a content identifier for identifying the
encrypted content and key type information showing a type of the content key, and
the generation unit generates the content key which corresponds to the encrypted content
identified by the content identifier and is of the type shown by the key type information.

23. (Original) The content playback device of Claim 19, wherein
key type information showing a type of the content key accompanies the encrypted
content on the recording medium,
the acquisition unit reads the key type information from the recording medium, and
the generation unit generates the content key of the type shown by the read key type
information.

24. (Original) The content playback device of Claim 23, wherein
the key type information is multiplexed with the encrypted content on the recording

medium, and

the acquisition unit separates the key type information from the encrypted content.

25. (Original) The content playback device of Claim 19, wherein the protection method information is stored on another recording medium, in correspondence with the encrypted content, and the acquisition unit acquires the protection method information by reading the protection method information from the other recording medium.

26. (Original) The content playback device of Claim 19, wherein the acquisition unit acquires the protection method information from another device that is connected to the content playback device via a network.

27. (Original) The content playback device of Claim 19, wherein the recording medium stores media information showing the media key, and the generation unit uses the media key shown by the media information.

28. (Original) The content playback device of Claim 27, wherein the media information includes the media key which has been encrypted using device information unique to the content playback device, and the generation unit reads the device information held in the content playback device, and decrypts the encrypted media key using the read device information to obtain the media key.

29. (Original) The content playback device of Claim 19, wherein the recording medium stores a contract identifier for identifying contract information which relates to the contract and shows the license key, in correspondence with the encrypted content, and the generation unit reads the contract identifier from the recording medium, and uses the license key shown by the contract information identified by the read contract identifier.

30. (Original) The content playback device of Claim 19, wherein the recording medium stores a content identifier for identifying the encrypted content, and

the generation unit reads the content identifier from the recording medium, and uses the license key corresponding to the content identifier.

31. (Original) The content playback device of Claim 19, wherein the generation unit includes:

a storage unit operable to store contract information including the license key, beforehand; and

a generating unit operable to read the contract information from the storage unit and generate the content key using the license key included in the read contract information, if the protection method information shows the second protection method.

32. (Original) The content playback device of Claim 19, wherein contract information including the license key is stored on another recording medium, in correspondence with the encrypted content, and

the generation unit reads the contract information from the other recording medium, and uses the license key included in the read contract information.

33. (Original) The content playback device of Claim 19 being connected, via a network, to a server device for delivering contract information including the license key, wherein

the generation unit receives the contract information from the server device, and uses the license key included in the received contract information.

34. (Original) The content playback device of Claim 19, wherein the recording medium stores content information unique to the encrypted content, in correspondence with the encrypted content, and

the generation unit generates the content key using the media key and the content information, if the protection method information shows the first protection method.

35. (Currently Amended) A content playback method for use in a content playback device for decrypting encrypted content recorded on a computer readable recording medium and playing back the decrypted content, comprising using a processor to perform the steps of:

- reading media information unique to the computer readable recording medium, from the computer readable recording medium;
- acquiring, from a source other than the computer readable recording medium, contract information relating to a contract for use of the encrypted content, and judging, based on the acquired contract information, whether the encrypted content is permitted to be used;
- receiving a designation of the encrypted content;
- acquiring protection method information showing one of a first protection method and a second protection method that is used for protecting the encrypted content;
- generating a content key, corresponding to the acquired protection method information, based on the read media information and the acquired contract information, if the encrypted content is judged as being permitted to be used;
- reading the encrypted content from the computer readable recording medium, and decrypting the encrypted content using the generated content key; and
- playing back the decrypted content, wherein
the encrypted content includes at least first-type encrypted content that is protected by the first protection method and second-type encrypted content that is protected by the second protection method different from the first protection method.

36. (Cancelled)

37. (Currently Amended) A computer program used in a computer for decrypting encrypted content recorded on a recording medium and playing back the decrypted content, the computer program stored in a computer readable storage medium, wherein the computer program, when executed, causes the computer to perform steps of:

- reading media information unique to the recording medium, from the recording medium;
- acquiring, from a source other than the recording medium, contract information relating to a contract for use of the encrypted content, and judging, based on the acquired contract information, whether the encrypted content is permitted to be used;

receiving a designation of the encrypted content;
acquiring protection method information showing one of a first protection method and a second protection method that is used for protecting the encrypted content;
generating a content key, corresponding to the acquired protection method information,
based on the read media information and the acquired contract information, if the encrypted content is judged as being permitted to be used;
reading the encrypted content from the recording medium, and decrypting the encrypted content using the generated content key; and
playing back the decrypted content, wherein
the encrypted content includes at least first-type encrypted content that is protected by the first protection method and second-type encrypted content that is protected by the second protection method different from the first protection method.

38-40. (Cancelled)

41. (Previously Presented) A computer readable recording medium storing:
first encrypted content protected by a first protection method and protection method information showing the first protection method, in correspondence with each other; and
second encrypted content protected by a second protection method different from the first protection method and protection method information showing the second protection method, in correspondence with each other.

42. (Original) The recording medium of Claim 41, wherein
the first protection method uses a media key assigned to the recording medium, and
the second protection method uses a license key assigned to a contract for use of the encrypted content.